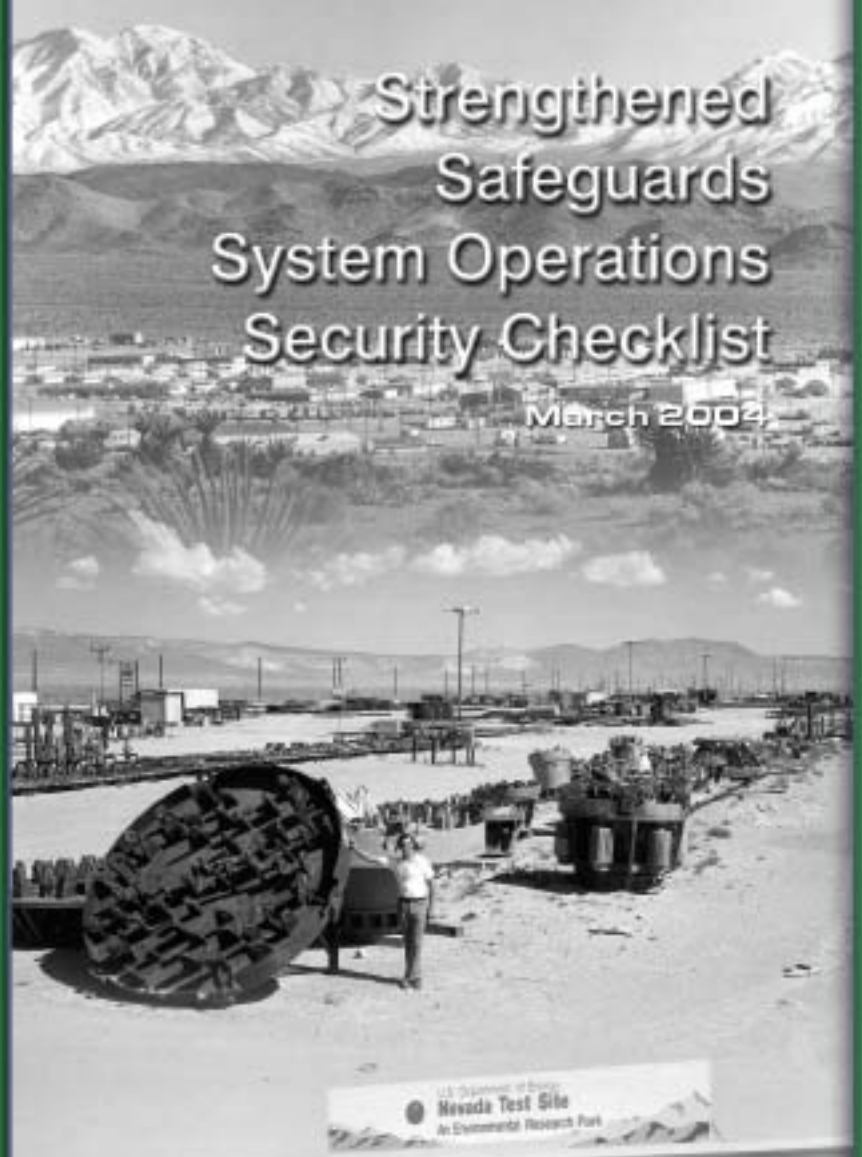
Distributed by:
Defense Threat Reduction Agency
DTIRP Outreach Program
8725 John J. Kingman Road, MSC 6201
Fort Belvoir, VA 22060-6201
1.800.419.2899
Email: dtirpoutreach@dtra.mil
Web: http://dtirp.dtra.mil

Order No. 608P
March 2004

Strengthened Safeguards System Operations Security Checklist

March 2004



U.S. – IAEA Safeguards Agreement

Order No. 608P

This pamphlet was prepared by the Defense Treaty Inspection Readiness Program (DTIRP) to help increase ***Readiness Through Awareness*** within the U.S. Government and defense contractor community. Additional copies of this pamphlet, as well as other information about arms control treaties and the application of security countermeasures, are available through the DTIRP Outreach Program.

March 2004

Prepared for:
Defense Threat Reduction Agency
DTIRP Outreach Program
8725 John J. Kingman Road, MSC 6201
Fort Belvoir, VA 22060-6201

From the DTIRP Outreach series: Order No. 608P

TABLE OF CONTENTS

INTRODUCTION

This checklist is designed to assist personnel conducting vulnerability assessments at sites eligible for declaration under the United States-International Atomic Energy Agency (IAEA) Strengthened Safeguards Agreement. Specifically, these assessments pertain to Department of Defense (DoD) facilities, programs, and activities collocated at sites operated by the Department of Energy (DOE) or Nuclear Regulatory Commission (NRC) licensees. The checklist generally follows the operations security (OPSEC) assessment format, and is divided into the following phases:

- Asset/Sensitive Information
- Susceptibility
- Threat
- Vulnerability
- Risk
- Probability
- Recommended Countermeasures

The asset/sensitive information phase focuses on DoD programs and activities, as well as national security, proprietary, and other sensitive information. Once a sensitive asset has been identified, the susceptibility phase addresses whether inspectors would have access to the DoD program or activity where the asset is located. If IAEA inspectors could have access to that area, the threat posed by the inspection team and their equipment is assessed.

The vulnerability phase determines whether existing protective measures would adequately prevent the collection of sensitive information by observation, sampling and analysis, or other inspection activities. Once asset vulnerability is determined, a risk assessment is undertaken. This involves reviewing the level of access permitted, as well as the inspection team's capabilities and motivation to collect information against DoD programs.

The probability phase examines many factors-including site history-to determine the likelihood of an inspection occurring. If it is highly probable that an inspection could occur, and if access to an asset is also likely, additional countermeasures or managed access procedures may be recommended to protect the asset during inspection activities. Whenever possible, recommended countermeasures should be transparent to an inspector.

CHECKLISTS

Asset/Sensitive Information

The first—and probably most difficult—step of the assessment process is the collection of information on assets and sensitive information for the purpose of identifying security concerns. This step is key to the rest of the assessment process. Time should be taken to understand a facility's programs and to collect information.

The location of each activity and every aspect of each program—both sensitive and unclassified—needs to be identified. Then it can be determined which programs and activities are sensitive. When making this determination, it is important to evaluate whether any single or cumulative amount of unclassified information indicates the presence of a sensitive program or activity.

To identify sensitive information, it is more timely and cost-effective to follow the program or activity to each location rather than inspecting every structure or area on a facility. When a number of sensitive programs or activities are present, collocation of activities from different programs and DOE inspectable areas can be noted. Plotting these program components on a site diagram may be useful for tracking activities, as will following the checklists in this pamphlet, which begin here.

- ❑ Determine the number of sensitive programs or activities.
- ❑ Identify the location of program activities and their subcomponents.
- ❑ Determine whether a program has proprietary information that must be protected.*
- ❑ Identify DoD equities collocated with declarable activities at the facility (Annex I and Annex II of the Strengthened Safeguards Agreement).

*Coordination with the Nuclear Safeguards Implementation Working Group (NSIWG) may facilitate determination.

- ❑ Where DoD equities reside, determine whether a facility or building engages in activities subject to inspection under the Strengthened Safeguards Agreement.*
- ❑ Determine whether a facility or building houses national security or other sensitive equities.*
- ❑ Identify records, reports, plans, or materials in the inspectable area relating to DoD equities.
- ❑ Identify observable, special, or unique equipment relating to DoD equities.
- ❑ Identify observable activities or operations indicative of DoD equities.
- ❑ Identify personnel whose presence or observable activities are related to—or are perceived to be related to—DoD equities.
- ❑ Identify unique or specialized materials or subcomponents relating to DoD equities.
- ❑ Identify unique or specialized safety or security procedures relating to DoD equities.
- ❑ Identify unique facility configurations or structures relating to DoD equities.
- ❑ Identify unique or specialized suppliers whose products or services relate to DoD equities.
- ❑ Identify solid, liquid, or gaseous waste products or by-products relating to DoD equities.
- ❑ Identify actual DoD activities collocated or in close proximity to declarable facilities or items.
- ❑ List each identified item by category and priority on a worksheet, and classify findings, as necessary.

*Coordination with the Nuclear Safeguards Implementation Working Group (NSIWG) may facilitate determination.

NOTES

Susceptibility

Some sensitive information may not be susceptible to inspection. Understanding inspector rights and obligations, as well as inspection modalities, will assist in determining whether an inspector will have a right to access the location where the sensitive information resides. Susceptibility will need to be determined at each location where a program or an element of an activity is present.

- ❑ For each DoD equity or sensitive indicator, determine the required inspector access for each collocated DOE declarable item.
- ❑ Determine inspector access to the DoD equity during their access to a declarable item.
- ❑ Specify the probable inspection activity related to each inspectable item and collocated equity or sensitive indicator (observation, measuring, sampling, etc.).
- ❑ Determine whether the DoD equity has any signature similar to items of inspection from Annex I or Annex II of the Strengthened Safeguards Agreement.

NOTES

Threat

IAEA inspectors will have significant technical expertise pertaining to the conduct of inspection and collection activities. It is important to assume that these inspectors will be capable of exploiting inspection activities against a DoD equity. Inspectors' nationalities and their national technology and program collection objectives should be determined when analyzing the threat.

- ❑ Determine the inspection team's capability for collecting information against DoD equities.
- ❑ Identify inspection equipment that could be used against declarable items.
- ❑ Determine whether inspection equipment could collect against DoD equities.
- ❑ Determine inspectors' interests in the program.
- ❑ Determine inspectors' objectives.
- ❑ Identify individual inspector's national programs that are similar to DoD equities.

NOTES

Vulnerability

To determine vulnerability, it is necessary to overlay: 1) the susceptible areas, 2) the presence of the threat (the inspectors), and 3) sensitive information. If susceptibility, threat, and sensitive information overlap, then vulnerability exists.

- ❑ Determine whether security classification guidance and physical security procedures adequately protect equities from collection by inspectors.
- ❑ Determine whether sensitive indicators are visible or vulnerable due to their location.
- ❑ Determine whether unclassified aspects of DoD equities are vulnerable to visual observation.
- ❑ Determine whether unclassified aspects of DoD equities are vulnerable to sample analysis.

NOTES

NOTES

Risk

From the information developed during the vulnerability analysis, it is possible to determine risk. If sensitive information is observable or can be revealed through sampling and analysis, risk is high. At each location of sensitive information it is necessary to determine whether inspection activities place programs or activities at risk.

- ❑ Determine whether inspectors will have access to DoD equities.
- ❑ Determine whether inspectors can collect against DoD equities without having physical access to them.
- ❑ Determine inspectors' motivation to collect against DoD equities.

Probability

- ❑ Determine the likelihood of an inspection occurring at the facility or within an activity or program.
- ❑ Determine the likelihood of inspectors having access to an area where DoD equities are located.
- ❑ Determine inspectors' motives for collecting against DoD equities (political, economic exploitation, etc.).
- ❑ Review the site's history with respect to activities of interest to inspectors.
- ❑ Determine whether any of the inspectors represent a national will to collect against DoD equities.

NOTES

Recommended Countermeasures

Countermeasures should be appropriate and cost-effective based on the determined level of risk. They include action controls and simple procedural changes to alter or eliminate the "who," "what," "where," or "how" that provides access to sensitive information. Other countermeasures are diversion, concealment, shrouding, or camouflage to disrupt or prevent inspector access to sensitive information. Counteranalysis measures prevent interpretation of sensitive information by presenting an observable condition or situation that diverts the inspector's attention.

- ❑ Determine the usefulness of action controls.
- ❑ Determine the effectiveness of countermeasures.
- ❑ Determine the value of counteranalysis measures.
- ❑ Determine whether selected countermeasures are transparent to the inspectors.
- ❑ Determine whether managed access procedures can be used.
- ❑ Assess all selected countermeasures to ensure they do not create additional vulnerabilities.

NOTES

RELATED MATERIALS

407C Arms Control Treaties Information
CD-ROM

408P Arms Control Agreements Synopses
Pamphlet

410P Quick Reference Guide to
Arms Control Inspection Timelines
Pamphlet

907P DTIRP Arms Control Outreach Catalog
Pamphlet

908V Facility Protection Through Shrouding
Video

930C The Arms Control OPSEC Process
Automated CD-ROM

936V Verification Provisions—Point and Counterpoint
Video

942C DTIRP Outreach Products on CD
CD-ROM

950V The Technical Equipment Inspection (TEI) Process
Video

954T Why TEI?
Trifold Brochure

NOTES

NOTES